DEPARTMENT OF THE ARMY
HEADQUARTERS, US ARMY ARMOR CENTER AND FORT KNOX
75 6TH AVENUE
FORT KNOX, KENTUCKY 40121-5717

REPLY TO
ATTENTION OF:

Expires 12 April 2009

IMSE-KNX-IMO   12 April 2007

MEMORANDUM FOR

Commanders, All Units Reporting Directly to This Headquarters
Commanders, Fort Knox Partners In Excellence
Directors and Chiefs, Staff Offices/Departments, This Headquarters

SUBJECT: Fort Knox Policy Memo No. 7-07 – Use of Pirated Software on Government
Computers

1. References.

   a. AR 25-2, Information Assurance, 14 November 2003.

   b. Fort Knox Acceptable Use Policy (AUP), FK Form 5063-E, January 2007.

2. Definition. Pirated software is copyrighted software that is copied without paying for it.

3. Purpose. Pirated software is still being found on computers on this installation. This
problem requires our immediate, collective attention. We must take actions to eliminate the use
of unauthorized computer software. Besides being illegal, "pirated" software exposes our
computers to viruses and spy ware, which can lead to the loss of valuable information. The only
software authorized for use on government-owned computers is software written or purchased by
the Government, distributed by higher headquarters, and specifically approved by the Designated
Approving Authority (DAA) for use at this installation.

4. Applicability. This policy applies to all Soldiers, civilians, and contractors using a computer
system connected to the Fort Knox Campus Area Network (CAN).

5. Responsibilities. Commanders will ensure that every Soldier and civilian of this command
understands that use of pirated computer software is illegal. The user, and possibly the
Government, can be held equally liable.

6. Policy. It is a direct violation of the above references and federal law to copy and install
software that is paid for by the Government and not approved/authorized for use on the Fort
Knox CAN by the DAA. The DOIM employs programs to monitor the network for pirated
software. When pirated software is detected on a government information system, a member of
the DOIM Information Assurance Office will contact the user's Information Assurance Security
Officer /Information Management Officer; user's commander/director; Fort Knox DAA;
Director, DOIM; and Chief, Information/Personnel Security Branch, DPTMS, via e-mail

IMSE-KNX-IMO
SUBJECT: Fort Knox Policy Memo No. 7-07 – Use of Pirated Software on Government
Computers

outlining the content found and the appropriate steps that need to be taken in order for the user
and the government information system to be allowed back on the network.

7.   Point of contact is the Installation Information Assurance Manager at 624-5782.

FOR THE COMMANDER:

MARK D. NEEDHAM
COL, AR
Garrison Commander

DISTRIBUTION:
A